Finding ECM friendly curves: A Galois approach

Sudarshan SHINDE

Institut de Mathématiques de Jussieu - Paris Rive Gauche

Motivation - ECM algorithm

Algorithm 1 ECM (H. Lenstra 1985)

INPUT : n with at least two different prime factors
OUTPUT : a non-trivial factor of n.

```
B ← B_n, m ← B!
while No factor is found do
    P ← (x, y) ∈ Z/nZ × Z/nZ and an elliptic curve E on Z/nZ such that and P ∈ E(Z/nZ).
    P_m ← [m]P = (x_m : y_m : z_m) mod n
    g ← gcd(z_m, n)
    if g ∉ {1, n} then return g
    end if
end while
```

Correctness

Idea

Let p be an unknown prime factor of n. If $\mathrm{ord}(\mathrm{P})$ in $\mathrm{E}(\mathbb{F}_p)$ divides $\mathrm{B}!$, then

$$(x_\mathrm{B} : y_\mathrm{B} : z_\mathrm{B}) \equiv (0 : 1 : 0) \bmod p.$$

In this case p divides $\gcd(z_\mathrm{B}, n)$.

Sufficient condition

$\#\mathrm{E}(\mathbb{F}_p)$ is $\mathrm{B}-$smooth i.e. all its prime factors are $< \mathrm{B}$.

Theorem (Hasse)

Let E be an elliptic curve and p be a prime. Then,

$$p + 1 - 2\sqrt{p} \leq \#\mathrm{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Probability of success

- ECM succeeds if $\#\mathrm{E}(\mathbb{F}_p)$ is $\mathrm{B}-$smooth.
- $\#\mathrm{E}(\mathbb{F}_p) \approx p$ (Hasse)

Theorem (Lenstra)

For $p > 3$, let $\mathrm{S}_p = \{s : |s - (p+1)| \leq \sqrt{p} \text{ and } s \text{ is } \mathrm{B}-\text{smooth}\}$. Then the probability ECM succeeds is at least $\frac{c}{\log(p)} \frac{\#S - 2}{2\sqrt{p} + 1}$.

In other words, probability that a particular curve succeeds is comparable with the probability of finding a B-smooth number in the interval $(p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$.

Improved ECM algorithm

Algorithm 2 Practical version of ECM

INPUT : n with at least two different prime factors
OUTPUT : a non-trivial factor of n.

$\mathrm{B} \leftarrow \mathrm{B}_n$, $m \leftarrow \mathrm{B}!$
while No factor is found **do**
  $\mathrm{E}/\mathbb{Q} \leftarrow$ an elliptic curve from a family and $\mathrm{P} \in \mathrm{E}(\mathbb{Q})$.
  $\mathrm{P}_m \leftarrow [m]\mathrm{P} = (x_m : y_m : z_m)$ mod n
  $g \leftarrow \gcd(z_m, n)$
  if $g \notin \{1, n\}$ **then return** g
  end if
end while

Idea of Montgomery

Question : What if $\#\mathrm{E}(\mathbb{F}_p)$ is even for all primes p?
Theorem : If m divides torsion order of $\mathrm{E}(\mathbb{Q})$ then m divides $\#\mathrm{E}(\mathbb{F}_p)$ for almost all p.

Montgomery heuristic

Definition

Let E be an elliptic curve, ℓ be a prime and B be a sufficiently large integer. We define empirical average valuation,
$\bar{v}_\ell(\mathrm{E}) = \frac{\sum_{p<\mathrm{B}}(\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))}{\#\{p<\mathrm{B}\}}$

Heuristic

Curves with larger average valuation are ECM-friendly.

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$
2. Brier and Clavier (2010) : Torsion points over $\mathbb{Q}(i)$
   $\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)) = \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)|p \equiv 1 \bmod 4) + \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)\,|\,p \equiv 3 \bmod 4)$

How to improve average valuation ?

Some ways

1. Montgomery (1985), Suyama (1985), Atkin et Morain (1993), Bernstein et al (2010) : Torsion points over $\mathbb{Q}$
2. Brier and Clavier (2010) : Torsion points over $\mathbb{Q}(i)$
   $\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)) = \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)|p \equiv 1 \bmod 4) + \frac{1}{2}\overline{v}_2(\#\mathrm{E}(\mathbb{F}_p)\,|\,p \equiv 3 \bmod 4)$
3. Barbulescu et al (2012) : Better average valuation without additional torsion points by reducing the size of a "specific" Galois group.

Preliminaries

Definition (m-torsion field)

Let E be an elliptic curve on $\mathbb{Q}$, m a positive integer. The m-torsion field $\mathbb{Q}(\mathrm{E}[m])$ is defined as the smallest extension of $\mathbb{Q}$ containing all the m-torsion points.

As $\mathrm{E}(\bar{\mathbb{Q}})[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $\mathrm{G} = \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ is always a subgroup of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Theorem (Serre)

Let E be an elliptic curve without complex multiplication.

- For all primes ℓ outside a finite set depending on E and for all $k \geq 1$, $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$
- For all primes ℓ and $k \geq 1$, the index $[\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q})]$ is non-decreasing and bounded by a constant depending on E and ℓ.

How to improve average valuation ?

Theorem (Barbulescu et al. 2012)

Let ℓ be a prime and E_1 and E_2 be two elliptic curves. If $\forall n \in \mathbb{N}, \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_1[\ell^n])) \simeq \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_2[\ell^n]))$ then $\bar{v}_\ell(\mathrm{E}_1) = \bar{v}_\ell(\mathrm{E}_2)$.

Thus in order to change the average valuation,
we must change $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n]))$ for at least one n.

How to improve average valuation ?

Theorem (Barbulescu et al. 2012)

Let ℓ be a prime and E_1 and E_2 be two elliptic curves. If $\forall n \in \mathbb{N}, \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_1[\ell^n])) \simeq \mathrm{Gal}(\mathrm{E}_2[\ell^n]))$ then $\bar{v}_\ell(\mathrm{E}_1) = \bar{v}_\ell(\mathrm{E}_2)$.

Thus in order to change the average valuation,
we must change $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n]))$ for at least one n.

Exemple

Family	Torsion	$\bar{v}_2$	Primes found between $2^{15}, 2^{22}$
Suyama	$\mathbb{Z}/6\mathbb{Z}$	$^{10}/_3$	4069
Suyama - 11	$\mathbb{Z}/6\mathbb{Z}$	$^{11}/_3$	4756 (16% more)

Suyama-11 is implemented in GMP-ECM.

Constructing torsion field - Division polynomials

Definition - Theorem

For an elliptic curve E and a an integer m, we define the m-division polynomial as

$$\Psi_{(\mathrm{E},m)}(X) = \prod_{(x_\mathrm{P},\pm y_\mathrm{P})\in \mathrm{E}[m]-O} (X - x_\mathrm{P}) \qquad \in \mathbb{Q}[X],$$

and the exact m-division polynomial as

$$\Psi^{\mathrm{exact}}_{(\mathrm{E},m)}(X) = \prod_{(x_\mathrm{P},\pm y_\mathrm{P})\text{of order } m} (X - x_\mathrm{P}) \qquad \in \mathbb{Q}[X].$$

We have $\deg(\Psi_{(\mathrm{E},m)}) = \frac{m^2+2-3\eta}{2}$ where $\eta = m \bmod 2$.

Example

Let $\mathrm{E} : y^2 = x^3 + ax + b$ then $\Psi_{(\mathrm{E},3)} = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$

Constructing prime-power torsion field

Given $\mathrm{E} : y^2 = x^3 + ax + b$ and a prime-power ℓ^n, we construct $\mathbb{Q}(\mathrm{E}[\ell^n])$ recursively :

Constructing $\mathbb{Q}(\mathrm{E}[\ell])$

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(x_1) \hookrightarrow \mathbb{Q}(x_1, x_2) \hookrightarrow \mathbb{Q}(x_1, x_2, y_1) \hookrightarrow \mathbb{Q}(x_1, x_2, y_1, y_2) = \mathbb{Q}(\mathrm{E}[\ell])$$

where the polynomials defining the extensions are ;

1. (An irreducible factor of) $\Psi_{(\mathrm{E},\ell)}$
2. An irreducible factor of $\Psi_{(\mathrm{E},\ell)}$ on $\mathbb{Q}(x_1)$.
3. $f_1(y) = y^2 - (x_1^3 + ax_1 + b)$.
4. $f_2(y) = y^2 - (x_2^3 + ax_2 + b)$

Once we have $\mathbb{Q}(\mathrm{E}[\ell^{n-1}])$, we construct $\mathbb{Q}(\mathrm{E}[\ell^n])$ by the same method using $\Psi^{\mathrm{exact}}_{(\mathrm{E},\ell^n)}$ over $\mathbb{Q}(\mathrm{E}[\ell^{n-1}])$.

Inverse Galois problem - Main theorem

Definition (Resolvent polynomial)

Let G be a subgroup of $\mathcal{S}_n$ and $\mathrm{F}(X_1, ..., X_n) \in \mathrm{K}[X_1, ..., X_n]$ such that $\mathrm{G} = \{\sigma \in \mathcal{S}_n | \mathrm{F}(X_{\sigma(1)}, ..., X_{\sigma(n)}) = \mathrm{F}(X_1, ..., X_n)\}$. For a polynomial P, we define the resolvent polynomial

$$\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})(X) = \prod_{\sigma \in \mathcal{S}_n / \mathrm{G}} (X - \mathrm{F}(\theta_{\sigma(1)}, ..., \theta_{\sigma(n)})),$$

where $\theta_1, ..., \theta_n$ are the roots of P in $\bar{\mathrm{K}}$

Theorem

Let $\mathrm{P}, \mathrm{G}, \mathrm{F}$ be as above. Then,

1. $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})(X) \in \mathrm{K}[X]$.
2. If $\mathrm{Gal}(\mathrm{P}) \subset \mathrm{G}$ then $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})(X)$ has a root in K and if $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})(X)$ has a *simple* root in K then $\mathrm{Gal}(\mathrm{P}) \subset \mathrm{G}$ upto conjugacy.

$\boxed{\text{The theorem over } \mathrm{K} = \mathbb{Q}(a_1, \ldots, a_n) \Rightarrow \text{inverse Galois problem.}}$

The particular case of division polynomials

$$\mathrm{Split}(\Psi_{(\mathrm{E},m)}) \subset \mathbb{Q}(\mathrm{E}[m])$$

Particular case

- $m = 2^2$: **Theorem :** For a Montgomery curve $(By^2 = X^3 + Ax^2 + x)$, $\mathrm{Gal}(\Psi_4) \neq \mathbb{Z}/4\mathbb{Z}$.
- $m = 3$ **Theorem :** For any curve, if Ψ_3 is irreducible and $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[3]/\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ then $\#\mathrm{Gal}(\Psi_3) = 16$.

Remark

When $\mathrm{P} = \Psi_{(\mathrm{E},\ell)}$ of degree $n = \frac{\ell^2-1}{2}$, we have $\deg(\mathrm{R}_\mathrm{G}) = [\mathcal{S}_n : \mathrm{G}] > [\mathcal{S}_n : \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})] >$ exponential(ℓ^2)

The division polynomial is not a random polynomial.

Algorithmic search of infinite families

Computer algebra approach

Idea : Formal construction of torsion field and sufficient condition that its Galois group is generic.

Sufficient condition : When all the following extensions have generic degrees.

$$
\begin{aligned}
\mathrm{K}_4 &= \mathbb{Q}(a,b)(x_1,x_2,y_1,y_2) = \mathbb{Q}(a,b)(\mathrm{E}[\ell]) \\
&\quad \Big|\ \mathrm{P}_4 = y^2 - (x_2^3 + ax_2 + b) \\
\mathrm{K}_3 &= \mathbb{Q}(a,b)(x_1,x_2,y_1) \\
&\quad \Big|\ \mathrm{P}_3 = y^2 - (x_1^3 + ax_1 + b) \\
\mathrm{K}_2 &= \mathbb{Q}(a,b)(x_1,x_2) \\
&\quad \Big|\ \mathrm{P}_2 = \text{a factor of } \Psi \text{ of degree } \tfrac{\ell^2-\ell}{2} \\
\mathrm{K}_1 &= \mathbb{Q}(a,b)(x_1) \\
&\quad \Big|\ \mathrm{P}_1 = \Psi \text{ of degree } \tfrac{\ell^2-1}{2} \\
\mathrm{K}_0 &= \mathbb{Q}(a,b)
\end{aligned}
$$

Test if the above four polynomials are irreducible.

Non-generic Galois image

Example :

Let $\mathrm{E} : y^2 = x^3 + ax + b$ be an elliptic curve. Then $\Psi_3 = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$. We consider a partition of 4 of length 2.

- For $[2, 2]$, we write,

$$x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2 = (x^2 + e_2x + e_1)(x^2 + f_2x + f_1)$$

  and equate the coefficients on both sides. We get a system of polynomial equations,

$$\left\{\begin{array}{l} e_2 + f_2 = 0 \\ e_2 f_2 + e_1 + f_1 = 2a \\ e_1 f_2 + e_2\, f_1 = 4b \\ e_1 f_1 = -1/3\, a^2 \end{array}\right. \Rightarrow \left\{\begin{array}{l} f_2 = -e_2 \\ f_1 = 2a + e_2 f_2 - e_1 \\ e_1 \left(e_2{}^2 + 2\,a - e_1\right) + \frac{1}{3}\, a^2 = 0. \\ e_2{}^6 + 4\,ae_2{}^4 + \frac{16}{3}\, e_2{}^2 a^2 - 16\, b^2 = 0 \end{array}\right.$$

Thus, if the polynomial $3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$ does not have a root, then the factorization pattern of Ψ_3 is not $[2, 2]$.

Algorithm

Algorithm 3 Finding families

INPUT : A prime ℓ

OUTPUT : Necessary polynomial conditions in a and b such that $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell]))$ is non-generic for an elliptic curve E over $\mathbb{Q}(a, b)$

1: **for** $i \in \{1, 2, 3, 4\}$ **do**
2: $\quad \mathrm{F}_i \leftarrow$ absolute polynomial of K_{i-1}
3: $\quad$ **for** $r \in$ partitions of $\deg(\mathrm{P}_i)$ **do**
4: $\quad\quad \mathrm{S}_{i,r} \leftarrow$ System of polynomial equations in a, b and a root of F_i arising from equating coefficients
5: $\quad\quad \mathrm{C}_{i,r} \leftarrow$ Triangulation of $\mathrm{S}_{i,r}$ (Resultant)
6: $\quad\quad\quad \triangleright$ Necessary for factorization pattern of P_i to be r.
7: $\quad$ **end for**
8: **end for**
9: **return** Set of $\mathrm{C}_{i,r}$

A unified presentation

Montgomery (1992) : "The table entries were found in an ad hoc manner, so I make no claim completeness."

Kruppa (2007) : "The choice of $\sigma = 11$, which surprisingly leads to higher average exponent.."

Barbulescu et al (2012) : ".. suggests that by imposing equations on the parameters a and d we can improve the torsion properties."

"..By trying to force one of these three polynomials to split, we found four families."

Case $l = 3$

Theorem

Let $\mathrm{E} : y^2 = x^3 + ax + b$ be a rational elliptic curve with $ab \neq 0$. Let Ψ_3 be its 3-division polynomial and Δ its discriminant. Then we have,

Fact. Pattern of Ψ_3	Condition(s)	index
$(1,1,2)$	C_1 and a 3-torsion point	24
$(1,1,2)$	C_1	12
$(1,3)$	$\mathrm{C}_{2'}$ or $[\mathrm{C}_2$ and a 3-torsion point$]$	8
$(1,3)$	C_2	4
$(2,2)$	C_3	6
(4)	C_4	3

$\mathrm{C}_1 = 27\,x^{12} + 594\,ax^{10} + 972\,bx^9 + 4761\,a^2x^8 + 14256\,abx^7 + \ldots +$
$324\,ab\left(587\,a^3 + 3456\,b^2\right)x - 5329\,a^6 + 162432\,b^2a^3 + 1492992\,b^4$
$\mathrm{C}_{2'} = x^{16} - 24bx^{12} + 6\Delta x^8 - 3\Delta^2$
$\mathrm{C}_2 = 3x^4 + 6ax^2 + 12bx - a^2$
$\mathrm{C}_3 = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$

$\mathrm{C}_4 = x^3 - 2\Delta$ i.e. the j of E is a cube.

From conditions to families of curves

Remark

For every case, we got the equations of type $\exists x \in \mathbb{Q}$ such that $\mathrm{C}(a, b, x) = 0$.

From surface to curve

$(a, b) \sim (as^4, bs^6)$ (Same elliptic curve over $\mathbb{Q}$), So essentially $\mathrm{C}(a, b, x)$ is a plane curve. Replacing a and b by $a(j)$ and $b(j)$ or by random linear polynomials in t, we obtain a curve $\mathrm{C}(a(t), b(t), x)$. This curve describes infinitely many elliptic curves having the same Galois image.

Classical results on curves

Let C be a non-singular curve of genus g. Then if,

- $g \geq 2$, C has finitely many points. [Faltings]
- $g = 0$, if there is a point, there are infinitely many.
- $g = 1$, if there is a point, C can be put in Weierstrass form with rank r.

From conditions to families of curves : Example

Let $\mathrm{E} : y^2 = x^3 + ax + b$ be an elliptic curve. We saw that if Ψ_3 factors into two quadratic factors then
$\mathrm{C} = 3x^6 + 12ax^4 + 16a^2x^2 - 48b^2$ has a root.

If we put $b = 2a$, we get $\mathrm{C} = 3x^6 + 12ax^4 + 16a^2x^2 - 192a^2$.

This curve is of genus 0. We get a parametrization

$$a(t) = \frac{27t^3(19t+2)^3}{(242t^2+54t+3)(271t^2+57t+3)^2} \text{ and } b(t) = 2a(t).$$

Computing the generic valuation of a family

Theorem

Let $\mathrm{E}_t : y^2 = x^3 + a(t)x + b(t)$ such that $\mathrm{Gal}(\mathbb{Q}(t)(\mathrm{E}_t[\ell])/\mathbb{Q}(t)) \subseteq \mathrm{H}$. If $\exists t_0 \in \mathbb{Q}$ such that $\#\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_{t_0}[\ell])/\mathbb{Q}) = \#\mathrm{H}$ then $\mathrm{Gal}(\mathbb{Q}(t)(\mathrm{E}_t[\ell])/\mathbb{Q}(t)) = \mathrm{H}$.

Proof

Let $\mathrm{E}_t : y^2 = x^3 + a(t)x + b(t)$ and $p = t - t_0$.

$$\begin{array}{ccccc}
\mathrm{Gal}(\mathbb{Q}(t)(\mathrm{E}_t[\ell])/\mathbb{Q}(t)) & \overset{\supseteq}{\longleftarrow} & \mathrm{Dec}(\mathfrak{p}) & \xrightarrow{\mathrm{eval}_{t=t_0}} & \mathrm{Gal}(\mathbb{Q}(\mathrm{E}_{t_0}[\ell])/\mathbb{Q}) \\
\downarrow \rho & & & & \downarrow \rho \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & & \xrightarrow{\qquad\qquad\supseteq\qquad\qquad} & & \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})
\end{array}$$

where Dec is defined below.

Let K be a Galois extension of $\mathbb{Q}(t)$. Let $p \in \mathbb{Q}(t)$ and $\mathfrak{p}$ be an ideal of K above p. We define $\mathrm{Dec}(\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) | \sigma(\mathfrak{p}) = \mathfrak{p}\}$.

Valuations for $\ell = 3$

We obtain $g = 0$ for all the families for $\ell = 3$.

Theorem

Let $\mathrm{E} : y^2 = x^3 + ax + b, ab \neq 0$ be a rational elliptic curve. Then the generic average valuation $\bar{v}_3(\mathrm{E})$ is ${}^{87}/_{128} \approx 0.68$, except when one the following cases occurs.

A parametrization	Example (a, b)	Valuation
a, b complicated.	$(5805, -285714)$	${}^{33}/_{16} \approx 2.06$
a, b complicated.	$(284445, 97999902)$	${}^{45}/_{32} \approx 1.41$
$a = 3t^2, b = {}^{-243t^6 + 162t^4 - 9t^2}/_{36}$	$(3, -11)$	${}^{27}/_{16} \approx 1.69$
$a = \frac{-192\, t^3 - 254803968}{t^4}, b = \frac{-t^6 - 5308416\, t^3 - 4696546738176}{3t^6}$	$(-254804160, -\frac{4696552046593}{3})$	${}^{27}/_{16} \approx 1.69$
$a = \frac{-36t(t+2)^3}{(t^2+4t+1)^2}, b = 2a$	$(\frac{-4608}{169}, \frac{-9216}{169})$	${}^{39}/_{32} = 1.22$
$a = \frac{27t^3(19t+2)^3}{(242t^2+54t+3)(271t^2+57t+3)^2}, b = 2a$	$(\frac{250047}{32758739}, \frac{500094}{32758739})$	${}^{69}/_{64} \approx 1.08$
$a = \frac{216}{(t^3-8)}, b = 2a$	$(\frac{-216}{7}, \frac{-432}{7})$	${}^{69}/_{128} \approx 0.54$

Cryptographic application

Popular parametrizations

- Montgomery $By^2 = x^3 + Ax^2 + x$ or $y^2 = x^3 + \frac{3-A^2}{3B^2}x + \frac{2A^3-3A}{27B^3}$
- Edwards $ax^2 + y^2 = 1 + dx^2y^2$ or $y^2 = x^3 + \frac{3-\alpha^2}{3\beta^2}x + \frac{2\alpha^3-3\alpha}{27\beta^3}$ where $\alpha = -2\frac{a+d}{a-d}$ and $\beta = \frac{4}{a-d}$.
- Hessian $y^2 + axy + by = x^3$ or $y^2 = x^3 + (-27a^4 + 648ab)x + (54a^6 - 1944a^3b + 11664b^2)$.

Goal

- **INPUT :** A number field K, a prime ℓ and $a(\alpha, \beta)$ and $b(\alpha, \beta)$.
- **OUTPUT :** Complete list of equations of negligible density necessary for non-generic valuation $\bar{v}_\ell(\mathrm{E}_{a,b})$.

Valuation $m = 4$, Montgomery curve

Theorem

Let $\mathrm{E} : By^2 = x^3 + Ax^2 + x$ be a rational elliptic curve with $B(A^2 - 4) \neq 0$. Then the generic average valuation $\bar{v}_2(\mathrm{E})$ is ${}^{10}/_{3} \approx 3.33$, except,

- If $A^2 - 4 \neq \square$ i.e. $\mathrm{E}(\mathbb{Q})[2] \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we note Ψ be the quartic factor of its 4-division polynomial. Then we have,

Fact. Pat. of Ψ	Condition(s)	Index	Valuation
$(2,2)$	$A = -2\frac{t^4-4}{t^4+4}$	24	${}^{10}/_{3} \approx 3.33$
(4)	$\frac{A\pm 2}{B} = \pm\square$ or $\frac{4B^2}{A^2-4} = -t^4$	12	${}^{11}/_{3} \approx 3.67$

- If $A^2 - 4 = \square$ i.e. if $A = \frac{t^2+4}{2t}$. Then we have,

Fact. Pat. of Ψ	Condition(s)	Index	Valuation
$(1,1,2)$	$A = \frac{t^4+24t^2+16}{4(t^2+4)t}$ and $B = -t(t^2+4)\square$	48	${}^{14}/_{3} \approx 4.67$
$(1,1,2)$	$A = \frac{t^4+24t^2+16}{4(t^2+4)t}$	24	${}^{23}/_{6} \approx 3.83$
$(2,2)$	$A = \frac{t^2+4}{2t}$ and $\frac{A\pm 2}{B} = \square$	24	${}^{13}/_{3} \approx 4.33$
$(2,2)$	$A = \frac{t^2+4}{2t}$	12	${}^{11}/_{3} \approx 3.67$

Modular forms approach

Theorem (Sutherland, Zywina)

Let E be an elliptic curve and $\mathrm{H} \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $-1 \in \mathrm{H}$. Then there exists a polynomial $X_{\mathrm{H}}(j, t)$ such that $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^n])/\mathbb{Q}) \subset \mathrm{H}$ if and only if $\exists t_0 \in \mathbb{Q}$ such that $X_{\mathrm{H}}(j(\mathrm{E}), t_0) = 0$.

Fast computations of X_{H}

[1] Jeremy Rouse and David Zureick-Brown, "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois" (2015)

- Complete description of possible 2-adic Galois images.

[2] Andrew Sutherland and David Zywina, "Modular curves of prime-power level with infinitely many rational points" (2017)

- Complete description of possible ℓ-adic Galois images contained in subgroups containing -1.

Example

Curve	$j(\mathrm{E})$	$\#\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[3])/\mathbb{Q})$	$\bar{v}_3$
$y^2 = x^3 - 336x + 448$	1792	12	$^{39}/_{32}$
$y^2 = x^3 - 7^2 \cdot 336x + 7^3 \cdot 448$	1792	6	$^{54}/_{32}$

The modular forms approach does not work for arbitrary H.

Example

Curve	$j(\mathrm{E})$	$\#\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[3])/\mathbb{Q})$	$\bar{v}_3$
$y^2 = x^3 - 336x + 448$	1792	12	$^{39}/_{32}$
$y^2 = x^3 - 7^2 \cdot 336x + 7^3 \cdot 448$	1792	6	$^{54}/_{32}$

The modular forms approach does not work for arbitrary H.

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

	$-1 \notin \mathrm{H}$	$-1 \in \mathrm{H}$
$l = 2$	[1]	[1], [2]
$l \neq 2$		[2]

Our contribution

Complete list of elliptic curves having non-generic Galois image not containing -1.

Let $\tilde{\mathrm{H}}$ be subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ containing -1 and let H be subgroup of $\tilde{\mathrm{H}}$ such that $\tilde{\mathrm{H}} = \langle \mathrm{H}, -1 \rangle$.

$$\begin{tikzcd}
\mathbb{Q}(t)(\mathrm{E}[\ell^n]) & \\
 & L_2 = \mathbb{Q}(t)(\sqrt{f}) \arrow[ul, "\mathrm{H}"'] \\
\mathbb{Q}(t) \arrow[uu, "\tilde{\mathrm{H}}"] \arrow[ur] &
\end{tikzcd}$$

Cryptographic applications

A criterion to choose curves

Notation : $s \sim t$ if $t - \sqrt{t} < s < t + \sqrt{t}$.

p is fixed and E varies (H. Lenstra)

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}) = \frac{1}{\mathcal{O}(\log p)} \mathrm{Prob}(\textit{a random integer } \sim p \textit{ is } \mathrm{B}\textit{-smooth}).$$

A criterion to choose curves

Notation : $s \sim t$ if $t - \sqrt{t} < s < t + \sqrt{t}$.

p is fixed and E varies (H. Lenstra)

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}) = \frac{1}{\mathcal{O}(\log p)} \mathrm{Prob}(\textit{a random integer } \sim p \textit{ is } \mathrm{B}\textit{-smooth}).$$

E fixed and p varies in $[n - \sqrt{n}, n + \sqrt{n}]$

Can we claim the following ?

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}) = \mathrm{Prob}(\textit{a random integer } \sim ne^{\alpha} \textit{ is } \mathrm{B}\textit{-smooth}).$$

A criterion to choose curves

Notation : $s \sim t$ if $t - \sqrt{t} < s < t + \sqrt{t}$.

p is fixed and E varies (H. Lenstra)

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}) = \frac{1}{\mathcal{O}(\log p)} \mathrm{Prob}(\textit{a random integer } \sim p \textit{ is } \mathrm{B}\textit{-smooth}).$$

E fixed and p varies in $[n - \sqrt{n}, n + \sqrt{n}]$

Can we claim the following ?

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}) = \mathrm{Prob}(\textit{a random integer } \sim ne^{\alpha} \textit{ is } \mathrm{B}\textit{-smooth}).$$

Definition

For E an elliptic curve and n, B two integers, $\alpha(\mathrm{E}, n, \mathrm{B}) \in \mathbb{R}$ is such that

$$\frac{\#\{p \sim n \mid \#\mathrm{E}(\mathbb{F}_p) \textit{ is } \mathrm{B}\textit{-smooth}\}}{\#\{p \mid p \sim n\}} = \frac{\#\{x \sim ne^{\alpha(\mathrm{E},n,\mathrm{B})} \mid x \textit{ is } \mathrm{B}\textit{-smooth}\}}{\#\{x \mid x \sim ne^{\alpha(\mathrm{E},n,\mathrm{B})}\}}.$$

Example

Let $\mathrm{E} : y^2 = x^3 + 3x + 5$ and $n = 2^{25}$. We compute α for usual values of B.

$\alpha(\mathrm{E}, n, 30)$	-0.79
$\alpha(\mathrm{E}, n, 60)$	-0.83
$\alpha(\mathrm{E}, n, 90)$	-0.82

Example

Let $\mathrm{E} : y^2 = x^3 + 3x + 5$ and $n = 2^{25}$. We compute α for usual values of B.

$\alpha(\mathrm{E}, n, 30)$	-0.79
$\alpha(\mathrm{E}, n, 60)$	-0.83
$\alpha(\mathrm{E}, n, 90)$	-0.82

Theorem (Barbulescu and Lachand (2016))

Let f be a quadratic homogeneous polynomial with certain properties.

$$\mathrm{Prob}(f(n), n \sim \mathrm{N} \textit{ is } \mathrm{B}\textit{-smooth}) = \mathrm{Prob}(n \textit{ of size } \mathrm{N}e^{\alpha(f)} \textit{ is } \mathrm{B}\textit{-smooth}).$$

Question : Can we make α independent of n and B ?

Definition

Let n and B' be integers. We define B' sifted part of n,

$$\mathrm{C}_{\mathrm{B}'}(n) = \frac{n}{\prod_{p \leq \mathrm{B}'} p^{\mathrm{v}_p(n)}}.$$

In order to render α independent of n and B, we let $n, \mathrm{B} \longrightarrow \infty$ and replace proportions by the density of Chebotarev. Let $\mathrm{B}' < \mathrm{B}$.

Montgomery heuristic

If $\mathrm{C}_{\mathrm{B}'}(x)$ and $\mathrm{C}_{\mathrm{B}'}(\#\mathrm{E}(\mathbb{F}_p))$ are of the same size then x and $\#\mathrm{E}(\mathbb{F}_p)$ have the same chances of being B-smooth.

Thus when B' and $x \to \infty$, we expect,

$$\alpha + \log(n) - \sum_{\ell} \bar{v}_\ell(x) \log(\ell) = \log(n) - \sum_{\ell} \bar{v}_\ell(\mathrm{E}) \log(\ell).$$

This prompts us to define the following.

Formal definition of $\alpha(\mathrm{E})$

Assuming the convergence for now,

Definition

Let E be an elliptic curve and ℓ a prime. Let $\alpha_\ell(\mathrm{E}) = (\frac{1}{\ell-1} - \bar{v}_\ell(\mathrm{E})) \log \ell$. We define,

$$\alpha(\mathrm{E}) = \sum_{\ell} \alpha_\ell(\mathrm{E}).$$

Existence and computation of $\alpha(\mathrm{E})$

Calculations of $\bar{v}_\ell(\mathrm{E})$ can be done explicitly using the image of ℓ^n-torsion field.

Generic case

Let E_g be such that for all primes ℓ and for all $k \geq 1$, we have $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_g[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. In this case, we get $\bar{v}_\ell(\mathrm{E}_g) = \frac{(\ell^3+\ell^2-2\ell-1)\ell}{(\ell+1)^2(\ell-1)^3}$ and numerically $\alpha(\mathrm{E}_g) \approx -0.811997734$.

Existence and computation of $\alpha(\mathrm{E})$

Calculations of $\bar{v}_\ell(\mathrm{E})$ can be done explicitly using the image of ℓ^n-torsion field.

Generic case

Let E_g be such that for all primes ℓ and for all $k \geq 1$, we have $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_g[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. In this case, we get $\bar{v}_\ell(\mathrm{E}_g) = \frac{(\ell^3+\ell^2-2\ell-1)\ell}{(\ell+1)^2(\ell-1)^3}$ and numerically $\alpha(\mathrm{E}_g) \approx -0.811997734$.

Non-generic cases

According to a theorem of Serre, for every elliptic curve without complex multiplication, there are only finitely many primes ℓ for which $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q})$ can be different than $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. Thus in this case, α differs by only finitely many terms in its defining series.

Existence and computation of $\alpha(\mathrm{E})$

Calculations of $\bar{v}_\ell(\mathrm{E})$ can be done explicitly using the image of ℓ^n-torsion field.

Generic case

Let E_g be such that for all primes ℓ and for all $k \geq 1$, we have $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}_g[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. In this case, we get $\bar{v}_\ell(\mathrm{E}_g) = \frac{(\ell^3+\ell^2-2\ell-1)\ell}{(\ell+1)^2(\ell-1)^3}$ and numerically $\alpha(\mathrm{E}_g) \approx -0.811997734$.

Non-generic cases

According to a theorem of Serre, for every elliptic curve without complex multiplication, there are only finitely many primes ℓ for which $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q})$ can be different than $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. Thus in this case, α differs by only finitely many terms in its defining series.

Remark

Serre also conjectured that for every prime $\ell > 37$, $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$. This enables us to compute α for any given curve effectively assuming the conjecture. Andrew Sutherland has verified this conjecture with the curves in Cremona database.

α : An efficient tool

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$: For these curves $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{16}{3}$. Thus,
$$\alpha_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}} = \alpha_{generic} + (14/9 - 16/3)\log(2) \approx -3.4355.$$
2. Suyama-11 family : For these curves, $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{11}{3}$ and $\bar{v}_3$ changes from $\frac{87}{128}$ to $\frac{27}{16}$. Thus,
$$\alpha_{Suyama-11} = \alpha_{generic} + (14/9 - 11/3)\log(2) + (87/128 - 27/16)\log(3) \approx -3.3825.$$

α : An efficient tool

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$: For these curves $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{16}{3}$. Thus,
$$\alpha_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}} = \alpha_{generic} + (14/9 - 16/3)\log(2) \approx -3.4355.$$
2. Suyama-11 family : For these curves, $\bar{v}_2$ changes from $\frac{14}{9}$ to $\frac{11}{3}$ and $\bar{v}_3$ changes from $\frac{87}{128}$ to $\frac{27}{16}$. Thus,
$$\alpha_{Suyama-11} = \alpha_{generic} + (14/9-11/3)\log(2) + (87/128-27/16)\log(3) \approx -3.3825.$$

Numerical experiments with α. ($n = 2^{25}$)

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005753	0.005126	889 %	10.89 %
$\mathrm{B}_2 = 100$	0.008892	0.03883	0.042573	378.8 %	9.63 %

2. Suyama-11

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005133	0.005743	1008 %	11.89 %
$\mathrm{B}_2 = 100$	0.008892	0.04013	0.04101	361%,	2.19%

Some other families

$j(t)$	$\alpha(\mathrm{E}_{j(t)})$
$\frac{(t^9+9t^6+27t^3+3)^3(t^3+3)^3}{(t^6+9t^3+27)t^3}$	-1.5873
$\frac{256(t^8+8t^6+20t^4+16t^2+1)^3}{(t^2+4)(t^2+2)^2t^2}$	-2.2176
$\frac{(t^8-16t^4+16)^3}{(t^4-16)t^4}$	-2.3908
$\frac{-16(t^{16}-16t^8+16)^3}{(t^8-1)t^{32}}$	-2.4486
$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}+230t^8+8t^6+12t^4-8t^2+1)^3}{(t^4-6t^2+1)^2(t^2+1)^4(t^2-1)^8t^8}$	-2.6219
$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}+230t^8+8t^6+12t^4-8t^2+1)^3}{(t^4-6t^2+1)^2(t^2+1)^4(t^2-1)^8t^8}$	-3.4355

Conclusion and open questions

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Conclusion and open questions

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Open questions

- Proving theoretically that α works.

Conclusion and open questions

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?

Conclusion and open questions

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?
- Generalising the above work over number fields. In the NFS algorithm for discrete logarithms, one can have to factor many integers of the form $a^4 + b^4$. In this case, we search families over $\mathbb{Q}(\zeta_8)$.

Conclusion and open questions

Theorem

There are only finitely many values of $\alpha(\mathrm{E})$. And the best among them is approximately -3.43.

Open questions

- Proving theoretically that α works.
- There are curves where 2-Galois and 3-Galois are generic however 6-Galois is not. To what extent can these curves be used for ECM ?
- Generalising the above work over number fields. In the NFS algorithm for discrete logarithms, one can have to factor many integers of the form $a^4 + b^4$. In this case, we search families over $\mathbb{Q}(\zeta_8)$.

Thank you !